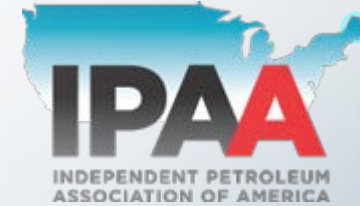


The Schlumberger logo is displayed in a large, bold, blue serif font. It is centered on a white rectangular background that has a subtle drop shadow, making it stand out against the blue gradient of the slide.

# MODERN MALWARE, MODERN DEFENSES AND PROTECTION

Mario Chiock, CISSP, CISM, CISA

[chiock@slb.com](mailto:chiock@slb.com)

# TAKEAWAYS

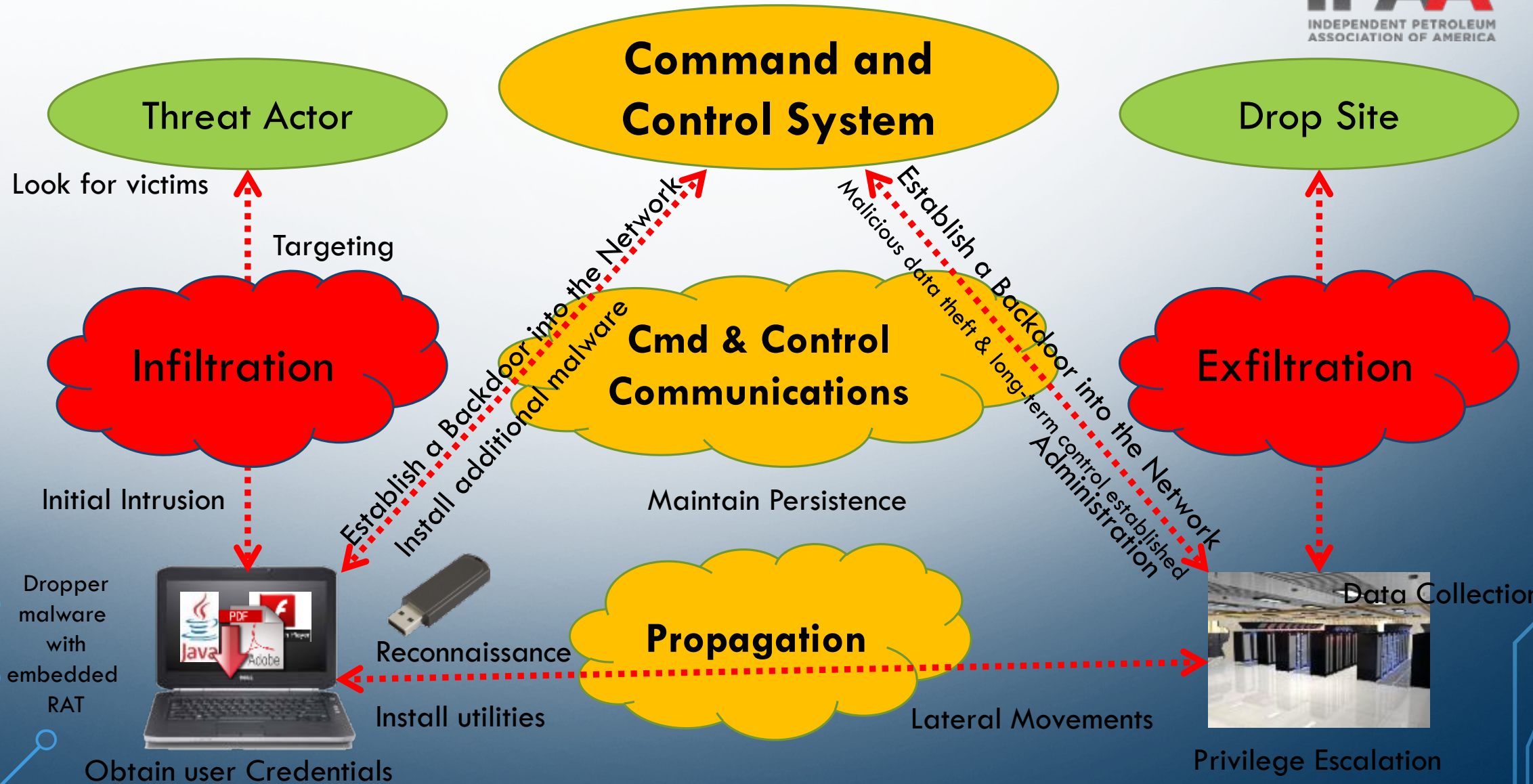
- Current Cybersecurity Landscape
- Recent data breaches / incidents
- Executive Order 13636 / Cybersecurity Framework
- Strategies to better protect the Oil & Gas industry

# Traditional Security is Insufficient



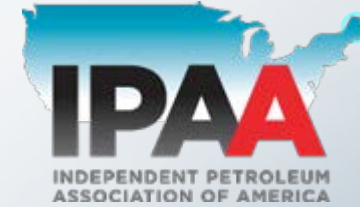


# LIFE CYCLE OF A MODERN ATTACK



# FIND TARGETS

- Google
- Wikipedia
- Zabasearch
- Shodan
- Robtex
- ZoomInfo
- Facebook
- Tweeter
- LinkedIn
- Yelp
- Google+
- Pinterest





# STEP ONE: **BAIT** AN END USER

- Use a Zero Day exploit



- Spear Phishing



- Social Media

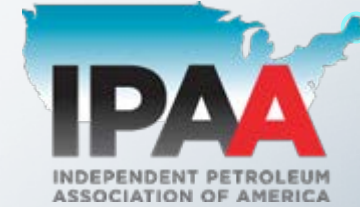


# STEP TWO : **EXPLOIT** A VULNERABILITY



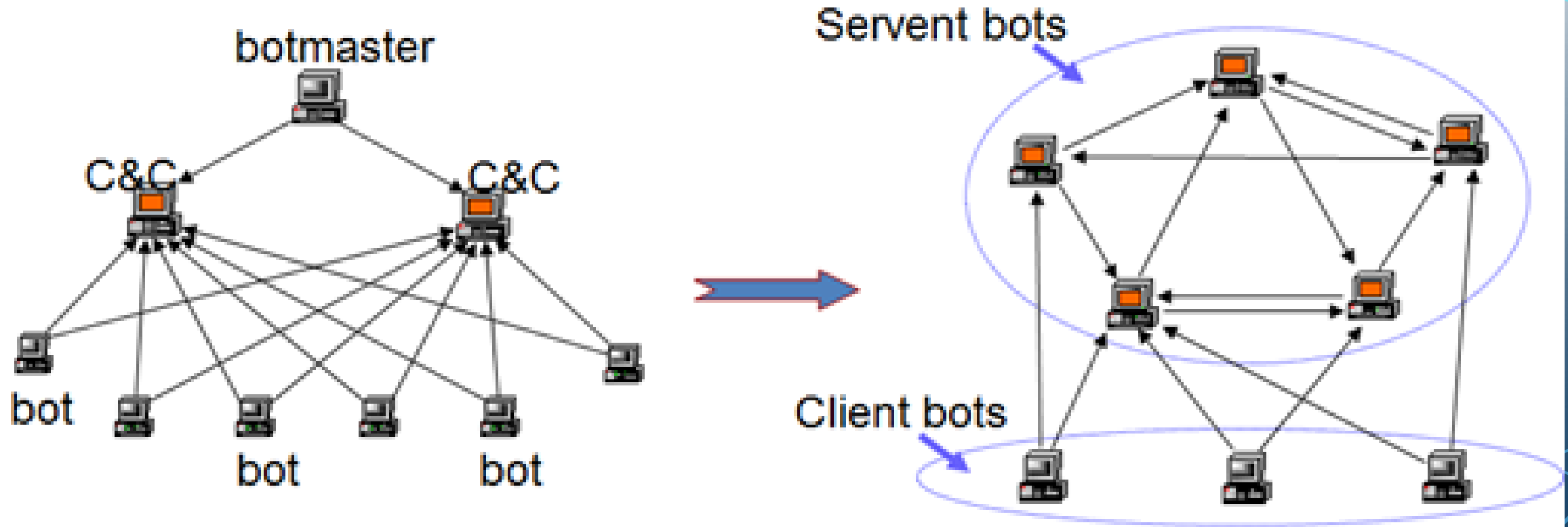


# STEP THREE: DOWNLOAD A **BACKDOOR**





# PEER-TO-PEER BOTNET



**From centralized botnet to hybrid peer-to-peer botnet**

# WHACK-A-MOLE SECURITY





If you did click– you are taken to a page with a number of embedded youtube videos:

As well as an iframe to an compromised site hosting a standard java/flash/PDF Swiss-army –style exploit kit :

```
<iframe width="640" height="360"
src="https://www.youtube.com/embed/046MuDipYJg">
</iframe>

<iframe width="640" height="360"
src="http://www.youtube.com/embed/H4Mx5qbgeNo">
</iframe>

<iframe width="640" height="360"
src="http://www.youtube.com/embed/JVU7rQ6wUoE">
</iframe>

<iframe width="640" height="360"
src="http://www.youtube.com/embed/RIHnpH2pFcv">
</iframe>

<iframe width="640" height="360"
src="http://www.youtube.com/embed/7ooIDyT2-Zs">
</iframe>

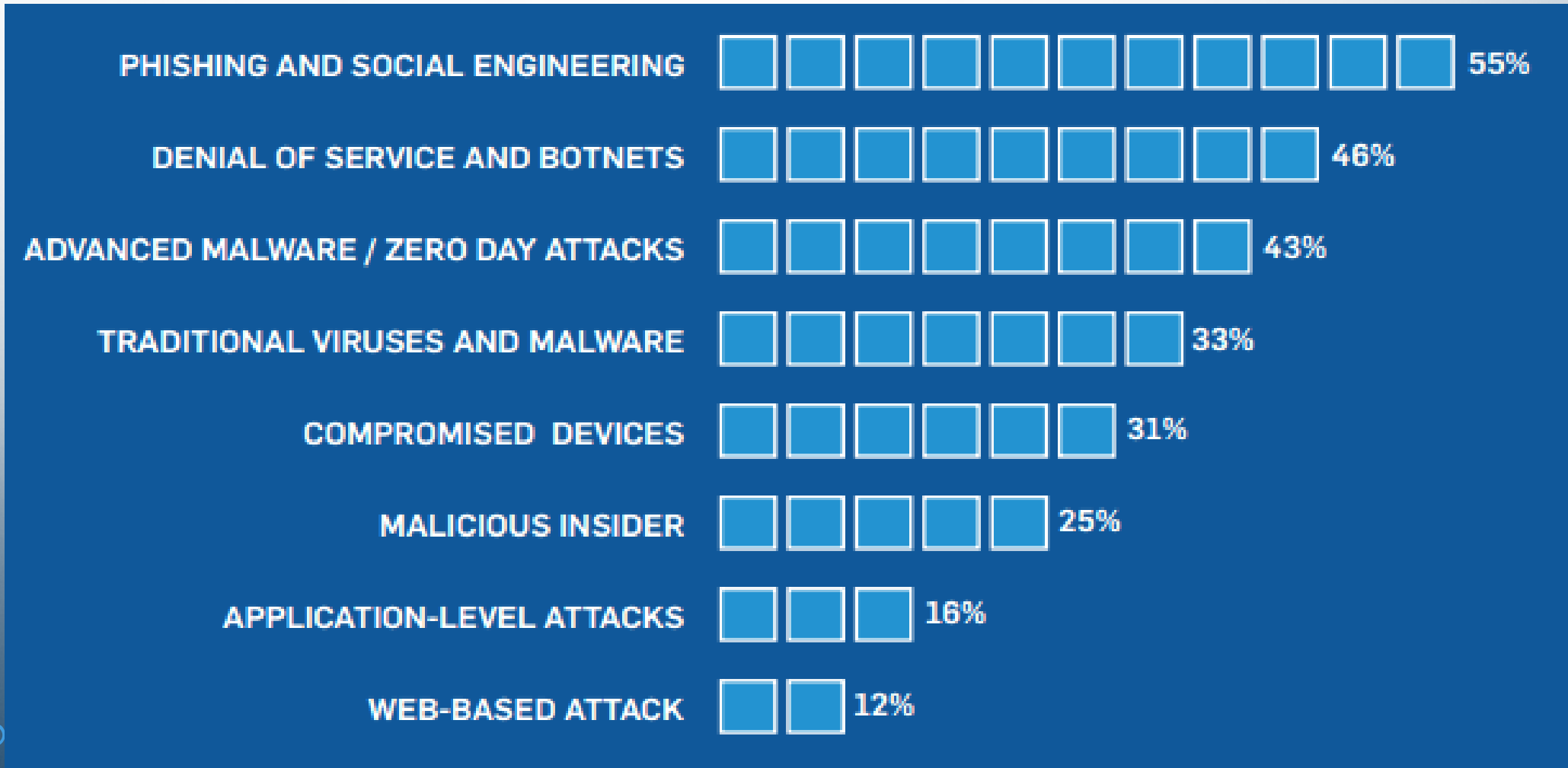
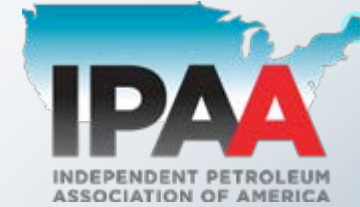
<iframe width="640" height="360"
src="http://pcdesires.com/hoiq.html">
</iframe>
```

Pcdesires.com should be DNS Sinkhole



–style exploit kit :

# MOST COMMON TYPES OF CYBER ATTACKS





# DATA BREACHES

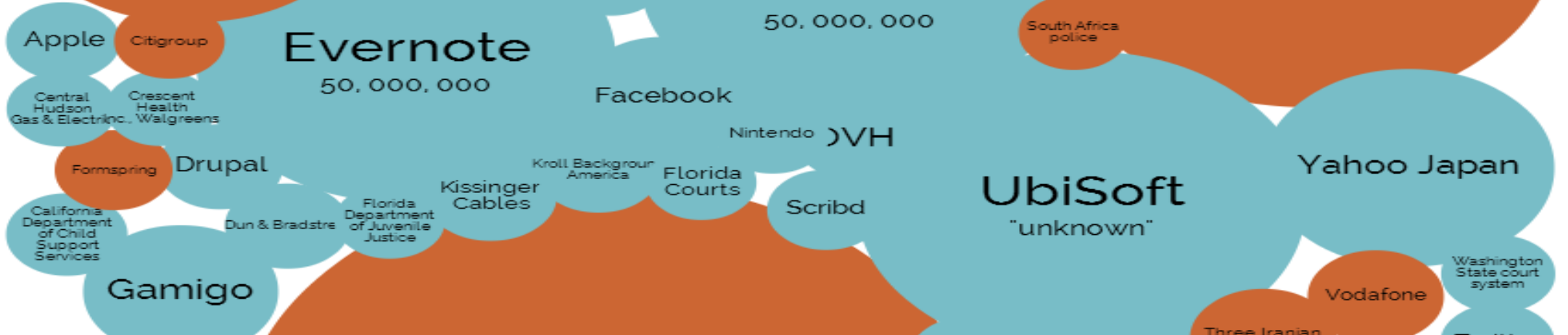


YEAR      BUBBLE COLOUR      YEAR      METHOD OF LEAK      BUBBLE SIZE      NO OF RECORDS STOLEN      DATA SENSITIVITY       SHOW FILE

latest



2013

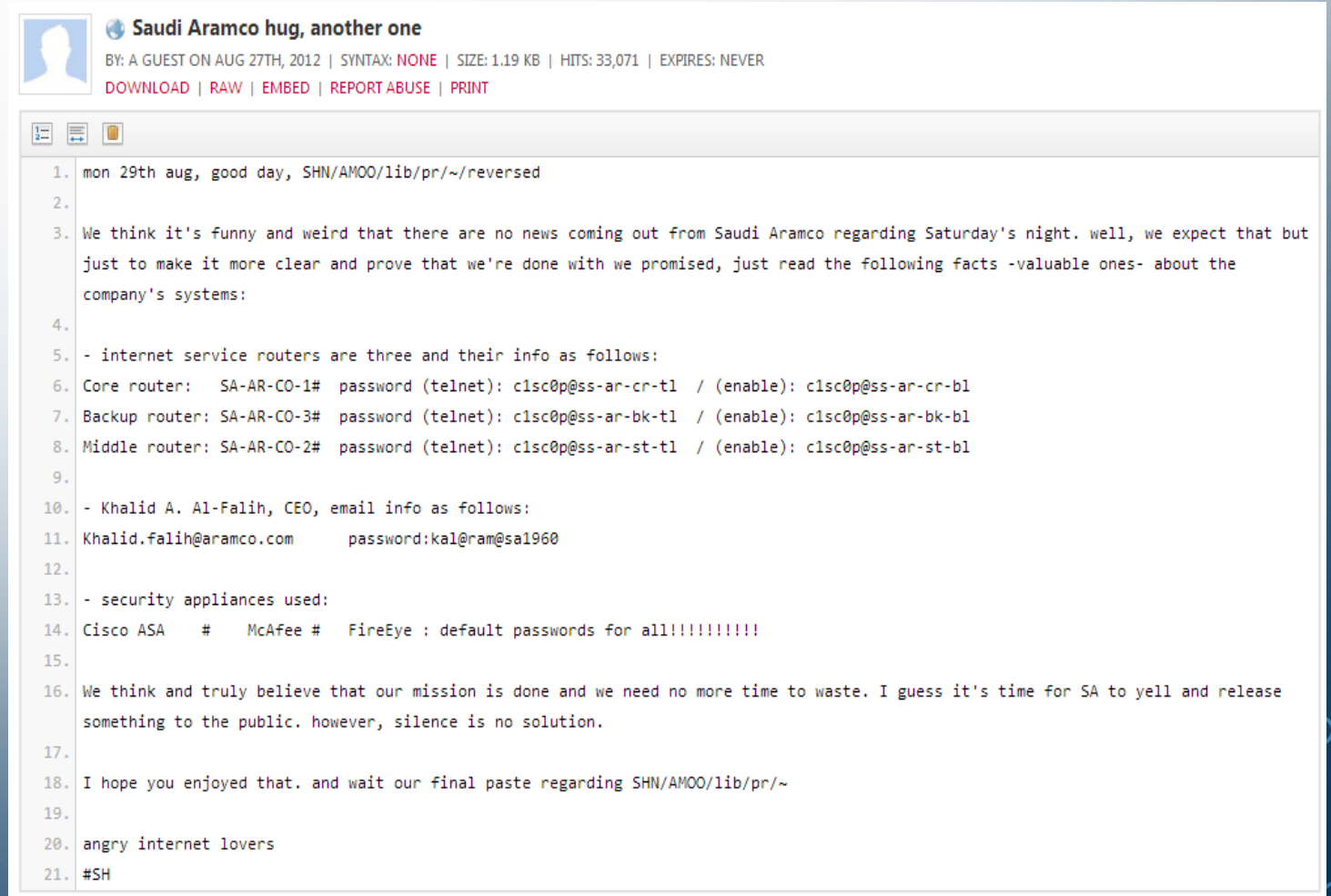


2012



# SAUDI ARAMCO - SHAMOON

- 30,000 machines
- Insider Exploiting privilege account
- Use of default passwords
- Use of share accounts



**Saudi Aramco hug, another one**  
BY: A GUEST ON AUG 27TH, 2012 | SYNTAX: NONE | SIZE: 1.19 KB | HITS: 33,071 | EXPIRES: NEVER  
[DOWNLOAD](#) | [RAW](#) | [EMBED](#) | [REPORT ABUSE](#) | [PRINT](#)

```
1. mon 29th aug, good day, SHN/AMOO/lib/pr/~ /reversed
2.
3. We think it's funny and weird that there are no news coming out from Saudi Aramco regarding Saturday's night. well, we expect that but
   just to make it more clear and prove that we're done with we promised, just read the following facts -valuable ones- about the
   company's systems:
4.
5. - internet service routers are three and their info as follows:
6. Core router: SA-AR-CO-1# password (telnet): c1sc0p@ss-ar-cr-t1 / (enable): c1sc0p@ss-ar-cr-b1
7. Backup router: SA-AR-CO-3# password (telnet): c1sc0p@ss-ar-bk-t1 / (enable): c1sc0p@ss-ar-bk-b1
8. Middle router: SA-AR-CO-2# password (telnet): c1sc0p@ss-ar-st-t1 / (enable): c1sc0p@ss-ar-st-b1
9.
10. - Khalid A. Al-Falih, CEO, email info as follows:
11. Khalid.falih@aramco.com password:kal@ram@sa1960
12.
13. - security appliances used:
14. Cisco ASA # McAfee # FireEye : default passwords for all!!!!!!!!!!!!
15.
16. We think and truly believe that our mission is done and we need no more time to waste. I guess it's time for SA to yell and release
   something to the public. however, silence is no solution.
17.
18. I hope you enjoyed that. and wait our final paste regarding SHN/AMOO/lib/pr/~
19.
20. angry internet lovers
21. #SH
```



# MALWARE THREATENING OFFSHORE RIG SECURITY

<http://fuelfix.com/blog/2013/02/25/malware-on-oil-rig-computers-raises-security-fears/>



Home Oil Field Pipelines Refining Power Washington Voices Jobs & Career Advice

## Malware threatening offshore rig security

Posted on February 25, 2013 at 7:01 am by Zain Shauk in Crude oil, Offshore

Malicious software unintentionally downloaded by offshore oil workers has incapacitated computer networks on some rigs and platforms, exposing gaps in security that could pose serious risks to people and the environment, cybersecurity professionals told FuelFix.

The worst-case scenario could be catastrophic: A malfunctioning rig and safety systems could cause a well blowout, explosion, oil spill and lost human lives, experts said.

Some of the infected files – from online sources featuring pornography or music piracy, for example – have been downloaded directly through satellite connections. But other malware was brought aboard on laptops and USB drives that were infected on land.

Companies can go a long way toward protecting their networks by keeping software up to date and taking other cyber-security measures. But some have been reluctant to invest in such services and remain vulnerable to the



Chevron's Genesis platform is shown in the Gulf of Mexico. (AP Photo/Mary Altaffer)

## Malware on oil rig computers raises security fears



31 August 2012 Last updated at 05:10 ET



## Computer virus hits second energy firm

Computer systems at energy firm RasGas have been taken offline by a computer virus only days after a similar attack on oil giant Aramco.

The attacks come as security experts warn of efforts by malicious hackers to target the oil and energy industry.

The attack forced the Qatar-based RasGas firm to shut down its website and email systems.

RasGas, one of the world's largest producers of liquid petroleum gas, said production was not hit by the attack.

The company said it spotted the "unknown virus" earlier this week and took desktop computers, email and web servers offline as it cleaned up.

The report comes only days after Saudi Arabia's Aramco revealed it had completed a clean-up operation after a virus knocked out 30,000 of its computers. The cyber- assault on Aramco also only hit desktop computers rather than operational plant and machinery.

Both attacks come in the wake of alerts issued by security firms about a virus called "Shamoon" or "Disstrack" that specifically targets companies in the oil and energy sectors.



Oil and energy firms are being targeted by a destructive virus say security researchers

### Related Stories

[Oil giant recovers from net virus](#)

[New virus targets energy sector](#)

[US probes power plant 'backdoor'](#)

### NEWS

## Exxon, Shell, BP hacked in Night Dragon attacks

Thursday 24 February 2011 09:19



Exxon Mobil, Royal Dutch Shell and BP were among the oil companies targeted by hackers working through internet servers in China, say US reports.

IT security firm McAfee reported on 10 February that the attacks had resulted in the loss of project-financing information relating to oil and gas field bids and operations.



McAfee said the attacks started in November 2009, but it did not identify the oil companies that were affected.

"We have identified the tools, techniques, and network activities used in these continuing attacks, which we have dubbed "Night Dragon," as originating primarily in China," McAfee said.

The hacked companies also include Marathon Oil, ConocoPhillips and Baker Hughes, according to Bloomberg, citing company sources and investigators who

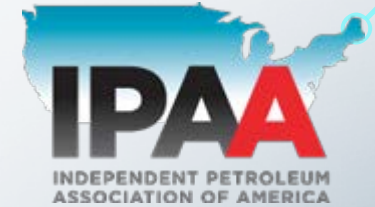
asked not to be identified because of the confidential nature of the matter.

In some of the cases, hackers had undetected access to company networks for more than a year, according to Greg Hogle, chief executive officer of security firm HBGary, which investigated some of the security breaches at oil companies.

Legal information, information on deals and financial information are all things that appear to be getting targeted, he said, describing the attacks as industrial espionage.



# HACKERS BREAK INTO CORPORATE SYSTEMS THROUGH VENDING MACHINES AND ONLINE RESTAURANT MENUS



<http://www.allgov.com/news/unusual-news/hackers-break-into-corporate-systems-through-vending-machines-and-online-restaurant-menus-140409?news=852874>

## Hackers Break into Corporate Systems through Vending Machines and Online Restaurant Menus



(AP photo)

With firewalls ever more difficult to breach, hackers have found other ways to sneak into protected computer systems, even those involving restaurant menus and soda machines.

When an employee uses his or her company computer to order food through an online menu, they can open up a cyber door for intruders to slip through and gain access to the local network of servers.

That's what happened to one unidentified oil company, *The New York Times* reported, when hackers attached malware to an online menu belonging to a Chinese restaurant frequented by the oil firm's employees. Simply browsing the menu resulted in the malicious code downloading into the user's computer and on to others at the corporation.

Vending machines set up in company break rooms also can provide a backdoor into a supposedly secure network. Many such machines contain minicomputers that allow the vendor to remotely

check on the supplies of soft drinks. But the same system can be utilized by hackers to infiltrate the computers of the company hosting the vending machines.

Printers, thermostats and videoconferencing equipment can also be vulnerable to intruders.

In other cases, hackers break in through a third-party's computer system, such as those providing heating and air conditioning at an office. This happened to retailer Target, which had its payment card system breached, potentially costing the company up to \$420 million in losses plus \$100 million to upgrade its system.

The third-party contractors usually don't have as a secure a computer network as their higher-end clients, yet in order to conduct business, those clients often allow the contractors access into their secure system. Piggybacking onto those more accessible third parties allows the hackers inside their primary targets' networks.

Top Stories

Unusual News

Where is the Money Going?

Controversies

U.S. and the World

Appointments and Resignations

Latest News

When Parents Die, Private

Military Judge Orders Release of  
Torture at Secret Prison

IRS Paid Bonuses to 1,100  
Didn't Pay Their Own Taxes

Two-Thirds of Criminals Released  
within 3 Years

Chinese Government Accused



# PHISHING STILL HOOKS ENERGY WORKERS

<http://fuelfix.com/blog/2013/12/22/phishing-still-hooks-energy-workers/>



Home Oil Field Pipelines Refining Power Washington Voices Jobs & Career Advice

## Phishing still hooks energy workers

Posted on December 22, 2013 at 6:30 am by Zain Shauk in Premium, Safety/Security

HOUSTON — The largest energy companies want their workers to stop clicking on links to cute cat photos.

Such emailed links are among the leading ways that hackers gain access to energy company systems — a trick known as phishing, with the potential for breaches that could lead to huge thefts of data, or even physical damage.

Phishing attackers try to get computer users to click on a link or download an attachment in an email that allows hackers to enter their systems.

In their latest counterattack, Schlumberger, Shell and other major players in the energy sector have been sending their employees fake phishing emails.

Unfortunately for many companies, employees are easily coaxed into clicking on bad links, said Jim Hansen, executive vice president for PhishMe, which specializes in phishing risks.

"Something as foolish as silly pictures of cats," Hansen said. "You think it's not going to happen. It always happens



(Fotolia for Frances)

# INSURERS WON'T COVER ENERGY COMPANIES BECAUSE THEIR CYBERSECURITY IS TOO WEAK

- <http://it-lex.org/insurers-wont-cover-energy-companies-cybersecurity-weak/>



eDiscovery » Featu...

**it-lex**  
Technology Law

IT-Lex Technology Law  
Eschewing tech law obfuscation to enlighten e...

HOME > DATA BREACHES > INSURERS WON'T COVER ENERGY COMPANIES BECAUSE THEIR CYBERSECURITY IS TOO WEAK

## Insurers Won't Cover Energy Companies Because Their Cybersecurity Is Too Weak

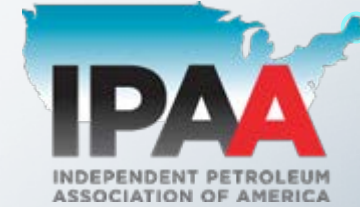
Date posted: *March 20, 2014* | Posted in *Data Breaches, Hacking, Security* | *0 comments*

A A A

DATA BREACHES



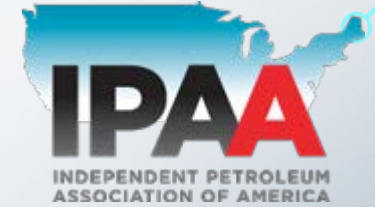
# EXECUTIVE ORDER 13636



- **Executive Order 13636**
  - Improving Critical Infrastructure Cybersecurity
- **Presidential Policy Directive (PPD)-21**
  - Critical Infrastructure Security and Resilience
- **NIST - Cybersecurity Framework (the Framework)**
- **DHS - The Critical Infrastructure Cyber Community – C3**
- **C2M2 - Cybersecurity Capability Maturity Model**

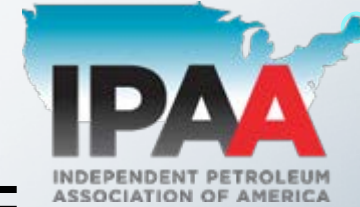


# **EXECUTIVE ORDER -- IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY ( FEBRUARY 12, 2013)**



- **Calls for improved cybersecurity**
- **Critical Infrastructure – Systems & Assets/ Virtual or Physical that could impact national security – Calls to enhance resiliency**
- **Policy Coordination – Follow Presidential Policy Directive 1 ( PPD1) of Feb. 13, 2009**
- **Cybersecurity Information Sharing – ISAC's**
- **Privacy and Civil Liberties Protections –**
- **Consultative Process – The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of Critical Infrastructure.**
- **Baseline Framework to Reduce Cyber Risk to Critical Infrastructure –**
- **Voluntary Critical Infrastructure Cybersecurity Program.**
- **Identification of Critical Infrastructure at Greatest Risk.**
- **Adoption of Framework**

# PRESIDENTIAL POLICY DIRECTIVE/PPD-21 CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

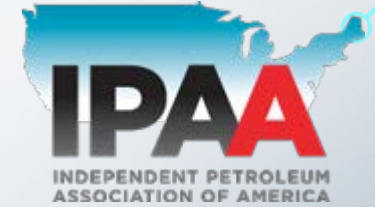


1. Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience;
2. Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and
3. Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.



# NIST CYBERSECURITY FRAMEWORK

[HTTP://WWW.NIST.GOV/CYBERFRAMEWORK/](http://www.nist.gov/cyberframework/)



NIST

[NIST Time](#) | [NIST Home](#) | [About NIST](#) | [Contact Us](#) | [A-Z Site Index](#)

Search

## Cybersecurity Framework

[About](#) [The Framework](#) ▾ [RFI](#) [Events](#)

[NIST Home](#) > [Cybersecurity Framework](#)

### Quick Links

[Executive Order 13636](#)

[Cybersecurity Framework \(PDF\)](#)

[Cybersecurity Framework \(EPUB\)](#)

[EPUB Help](#)

[Roadmap \(PDF\)](#)

[Cybersecurity Framework Core \(Excel\)](#)

[Alternative View: Appendix A – Framework Core Informative References \(PDF\)](#)



Executive Order 13636: Cybersecurity Framework

### Contact

[General Comments and Questions](#)

### Additional Information

- [Status Updates](#)

### Welcome

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the President issued Executive Order 13636, [Improving Critical Infrastructure Cybersecurity](#), in February 2013. It directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure.



# NIST CYBERSECURITY FRAMEWORK




Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

# DHS - THE CRITICAL INFRASTRUCTURE CYBER COMMUNITY – C3

[HTTP://WWW.US-CERT.GOV/CCUBEDVP](http://www.us-cert.gov/ccubedvp)



 Official website of the Department of Homeland Security



## US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

[HOME](#)

[ABOUT US](#)

[PUBLICATIONS](#)

[ALERTS AND TIPS](#)

[RELATED RESOURCES](#)

[C<sup>3</sup> VP](#)



### Critical Infrastructure Cyber Community Voluntary Program

[About](#)

[Getting Started](#)

[Getting Started for Business](#)

[Getting Started for Federal Government](#)

[Getting Started for SLTT Government](#)

[Self Service Tools](#)

## Critical Infrastructure Cyber Community Voluntary Program

As part of Executive Order (EO) 13636, the Department of Homeland Security (DHS) launched the Critical Infrastructure Cyber Community or C<sup>3</sup> (pronounced "C Cubed") Voluntary Program to assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (the Framework), released in February 2014. The C<sup>3</sup> Voluntary Program was created to help improve the resiliency of critical infrastructure's cybersecurity systems by supporting and promoting the use of the Framework. To contact us, please email us at [ccubedvp@hq.dhs.gov](mailto:ccubedvp@hq.dhs.gov).

The C<sup>3</sup> Voluntary Program Outreach and Messaging Kit includes informational materials provided in PDF format for easy printing and/or electronic distribution to help educate stakeholders about the C<sup>3</sup> Voluntary Program.

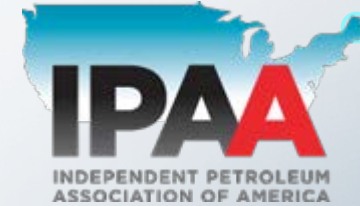
Access the C<sup>3</sup> Voluntary Program Outreach and Messaging Kit.

On This Page:  
[About the C<sup>3</sup> Voluntary Program](#)  
[C<sup>3</sup> Voluntary Program Activities](#)



# CYBERSECURITY CAPABILITY MATURITY MODEL

[HTTP://ENERGY.GOV/OE/CYBERSECURITY-CAPABILITY-MATURITY-MODEL-C2M2](http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2)



## OIL AND NATURAL GAS SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ONG-C2M2)

The Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2) was established as a result of the Administration's efforts to improve electricity subsector cybersecurity capabilities, and to understand the cybersecurity posture of the energy sector. The ONG-C2M2 includes the **core C2M2** as well as additional reference material and implementation guidance specifically tailored for the oil and natural gas subsector. The ONG-C2M2 comprises a maturity model, an evaluation tool, and DOE-facilitated self-evaluations.

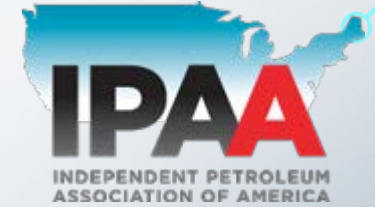
The ONG-C2M2 provides a mechanism that helps organizations evaluate, prioritize, and improve cybersecurity capabilities. The model is a common set of industry-vetted cybersecurity practices, grouped into ten domains and arranged according to maturity level. The ONG-C2M2 evaluation tool allows organizations to evaluate their cybersecurity practices against ONG-C2M2 cybersecurity practices. Based on this comparison, a score is assigned for each domain. Scores can then be compared with a desired score, as determined by the organization's risk tolerance for each domain.

Facilitated self-evaluations provide organizations with an opportunity to conduct ONG-C2M2 evaluations with the aid of experienced facilitators in a one-day structured walk-through. Facilitators guide discussions, answer questions, and clarify model concepts to increase the accuracy of an evaluation.

The model is publicly **available** and can be used by any organization to enhance its cybersecurity capabilities. More information is available in the **FAQs**. For organizations performing self-assessments, a **C2M2 Facilitators Guide** and C2M2 toolkit are available.

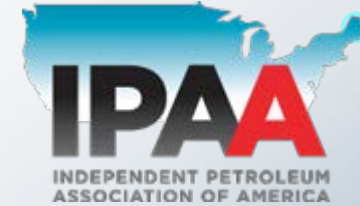


# STRATEGIES TO BETTER PROTECT THE OIL & GAS INDUSTRY



- Upgrade defenses with next-generation tools
- Layer protection base on need (example segment ICS from corporate network)
- Protect your data at rest ( HD Encryption / Digital Rights Management )
- Use Multi Factor authentication - Passwords alone no longer secure
- Invest on Preparedness
- Join the ONG-ISAC
- Manage Privilege access

# QUICK LOW COST SOLUTIONS & COUNTERMEASURES



- Remove Privilege access from users
- DNS sinkhole (<http://handlers.sans.edu/gbruneau/sinkhole.htm> )
- Enable UAC ( User Account Control ) to max
- Enable / use AppLocker
- Block execution of tools like PsExec, PsLoggedOn, PsService & PsInfo
- Browser Check (<https://browsercheck.qualys.com> )
- SNORT (<http://www.snort.org> )
- Implement SPF (Sender Policy Framework - <http://www.openspf.org> )



## WHAT ELSE CAN WE DO ?

- Use Application white listing ( Antivirus is not effective )
- Careful with your 3<sup>rd</sup> Party
- User Next-Generation tools ( NGFW – Next-Gen Threat prevention )
- Phishing – Social Engineering
- Invest in Preparedness First, Training & Awareness, Prevention
- Encrypt your Hard Drive
- Use Data Centric protection (Digital Rights Management)
- Watermark & Fingerprint highly sensitive documents





# USEFUL ORGANIZATIONS TO JOIN

- InfraGard – <https://www.infragard.org/>
- ISSA – <http://www.issa.org/>
- ISACA – <https://www.isaca.org>
- ICS-CERT
- US-CERT
- STOP-Think-Connect (<http://www.dhs.gov/stopthinkconnect>)





# WATCH OUT FOR

- **Mobile devices malware**
- **Industrial controls Systems**
- **Automation equipment (Drilling Automation)**
- **Vehicles**
- **Internet of things**
- **Medical devices**

